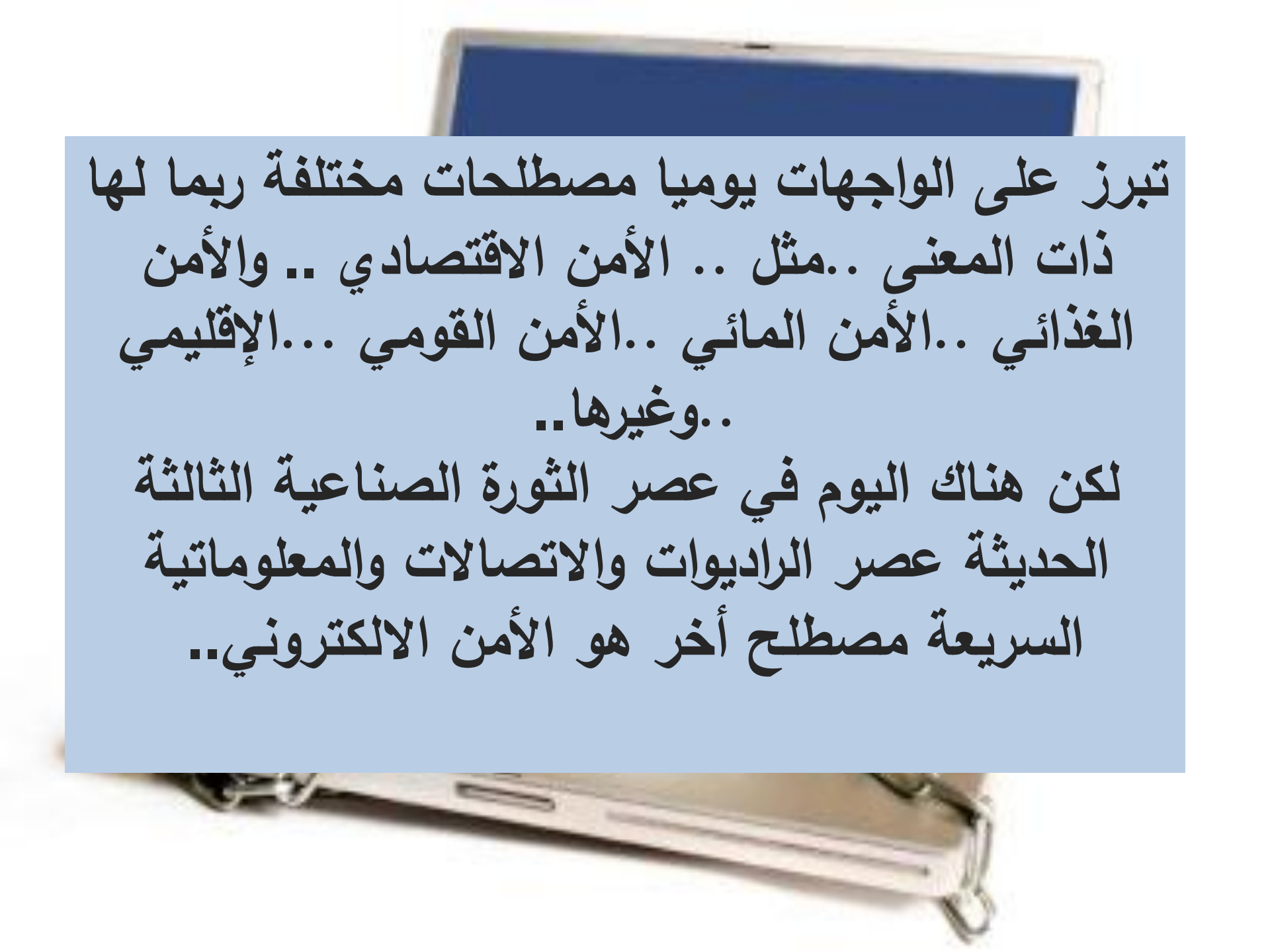
الأمن الالكتروني



تبرز على الواجهات يوميا مصطلحات مختلفة ربما لها ذات المعنى ..مثل .. الأمن الاقتصادي .. والأمن الغذائي ..الأمن المائي ..الأمن القومي ...الإقليمي ..وغيرها..

لكن هناك اليوم في عصر الثورة الصناعية الثالثة الحديثة عصر الراديوات والاتصالات والمعلوماتية السريعة مصطلح أخر هو الأمن الالكتروني..

هذا المصطلح ربما لا يختلف عن غيره من المصطلحات أعلاه وواضح ان ثمة خطر الكتروني يهدد المعلومات الشخصية والمؤسساتية وحتى الحكومية والقضايا الحساسة والتي ترتبط الكترونية ليكون خزنها والوصول اليه من ضمن تقنيات والاتصالات الحديثة.

اكبر خطر يهدد الأمن الالكتروني للمعلومات هو ظاهرة القرصنة وجرائم الانترنت ...لهذا الأمر سنت الكثير من الدول قوانين صارمة بحق جرائم الانترنت والقرصنة وحتى ما يعرف بالعبث الكتروني من إرسال فيروسات مدمرة لحواسيب وملفات الآخرين او سرقتها ونشرها بصورة غير قانونية او دون علم او موافقة أصحابها..

الأمن الالكتروني تطور كثيرا مع كثرة الاعتماد على الانترنت والاتصالات الشبكية الأخرى في تخزين ومعالجة والمعلومات والبيانات ..

في الولايات المتحدة الأمريكية الراعي الأكبر لأكبر عملاق لشركات الانترنت ومحركات البحث تقوم الدولة بسن قوانين مثلا لقوة التشفير للملفات المؤسساتية المختلفة وتصنيفها الى حسب أهميتها مثل تجاري وشخصي وحكومي..

وبرزت في الجانب التجاري للمصارف والبنوك والشركات تحديدا شكاوى كثيرة تطالب الحكومة الأمريكية بزيادة قوة التشفير للمعلومات الخاصة بملفات العملاء وحساباتهم وبيانات أخرى بخصوص حجم التداولات والصفقات وكيف تدار المؤسسة تلك او غيرها..

الحكومة الأمريكية ردت في كثير من الأحيان ان قوة التشفير الحالية كافية وقوية جدا لعدم تمكن القراصنة ومجرمي الانترنت من الوصول الى المعلومات..
في المقابل الشركات تصر على ان قوة التشفير المتاحة لهم غير كافية وان معلوماتهم مهددة بالخطر ويطالبون بزيادة تلك القوة .لكن الحال بقي على ما هو عليه..

لذا كان في المقابل قامت الكثير من الشركات وأصحاب المصالح الكبيرة بالاعتماد على شركات متخصصة للأمن ا لاكتروني..

تقوم هذه الشركات بحماية بيانات عملائها وتعقب مجرمي الانترنت الذي يحاولون القرصنة..

في الآونة الأخيرة ومن خلال التقارير الفصلية التي تصدرها بعض الشركات المتخصصة بالأمن الالكتروني كشفت عن زيادة كبيرة في نشاط مجرمي الانترنت..

من خلال تعقبهم ومعرفة طرقهم واهم البرامج التي يعتمد هؤلاء الهكر في عملياتهم وجد أنهم يعلمون مع أكثر الشركات الناجحة بحيث يعرضون خدماتهم في ان يقوموا هم في حماية شركات شرعية من إعمال القرصنة وبالمقابل يمارسون نشاطهم الغير مشروع في معرفة أهم الإستراتيجيات المستخدمة من قبلهم لحماية ملفات تلك الشركات وتكوين تحالف بين هؤلاء الهكر وتلك الشركات في تبادل الخبرات والبرامج والتقنيات المستخدمة للحد من إعمال القرصنة ..وبالتالي يحصل هؤلاء الهكر على إرباح طائلة من تلك الشركات..
كيف يحصل الهكر ومجرمي الانترنت على إرباح طائلة من شركات شرعية يتحالفون معها..

هؤلاء الهكر بعرفة اهم الاستراتيجيات المستخدمة في الكثير من الشركات الكبرى التي يتحالفون معها لحمايتها ومن خلال استعارة تلك الاستراتيجيات والتقنيات يقوم هؤلاء بتطوير أنظمة تجسس أقوى منها او معرفة أهم عيوبها ونقاط الضعف والثغرات فيها ..ثم يعرضون طرق جديدة لمكافحة وإصلاح تلك الثغرات والعيوب ..مقابل الحصول على مبالغ ضخمة من المال ..هؤلاء المجرمون يقومون أيضا بتطوير أنظمة اختراق معقدة لشبكات شركات أخرى والحصول على البيانات الشخصية منها ذات القيمة الجيدة بالنسبة لهم

بالإضافة الى معرفة أهم استراتيجيات الدفاع والعيوب فيها وتصميم أنظمة الاختراق كذلك لوحظ ان هؤلاء.
المجرمون يقومون بالإضافة في ألقاء شباكهم الواسعة على بيانات الغير يستخدمون ذكاؤهم الحاد في تجنب كشفهم من قبل الشركات المتخصصة بالأمن الالكتروني وكذلك الأنظمة المستخدمة للحماية.

كذلك معروف ومن زمن ربما طويل ان هؤلاء القراصنة والمجرمون لديهم شبكة علاقات واسعة فيما بينهم يتبادلون من خلالها معلوماتهم عن أهم الأنظمة الجديدة التي تستخدم للحماية واهم وأخر ابتكاراتهم في سبيل اختراق تلك الأنظمة ..لذا يلاحظ ان تطور هؤلاء المجرمون يتم بصورة سريعة ومعقدة جدا..

تقوم الكثير من شركات الحماية بتقديم مجموعة من توصياتها في عملها وتقاريرها ذات الصلة وذلك من حلال الحث على استخدام تقنيات متطورة للحماية والتعامل مع شركات معروفة بحسن السمعة في هذا المجال ولم ترصد لها مخالفات او اختراق من قبل كذلك تقدم مجموعة من أهم أساليب مجرمي الانترنت والمعلوماتية واهم أساليبهم في الاختراق وكيفية أعمالهم ..وحتى نوعية الملفات المستهدفة مثل بيانات العملاء وأرقام الحسابات وسرقة الأموال الشخصية وحتى العامة

كذلك من هذه التوصيات ((بدمج العقل البشري)) وأخر مبتكراته مع أخر معطيات العلم والتكنولوجيا كحل رئيسي لدرء إخطار هؤلاء المجرمون لأنهم وان كانوا يستخدمون تقنيات متطورة في الاختراق الان ان العقل البشري هو من يشغلها حسب رغبة هؤلاء ونوع العمل المراد العبث به من قبلهم والغاية منه والأهداف والدوافع له ...لذلك استخدام او دمج العقل البشري في عمليات الحماية والدفاع مع طرق التكنولوجيا من العوامل المهمة في معرفة أسلوب عمل مجرمي الانترنت لا الاعتماد على برامج وتقنيات تعمل آليا ..حيث يمكن خداعهما والتمويه لها بسهوله وبالتالي المرور منها واختراقها بسهولة من قبل الهكر.

أيضا في مجال الأمن الالكتروني يدخل اليوم جانب مهم في معرفة اخطر التهديدات في الانترنت وهي البرامج الخبيثة المسماة wormالمتسلسلة ..وايضا تهديدات المتمثلة بتقنيات botnetsوهي شبكات من أجهزة الكومبيوتر متخصصة لإحداث الضعف والضرر كوسيلة ناجحة من قبل مجرمي الانترنت والشبكيات كوسيلة فعالة لإطلاق هجماتهم المدمرة

وتحاول شركات الأمن الالكتروني لجذب اكبر قدر من المتعاونين معها من نفس هؤلاء المجرمين حيث ان معروف عنهم حبهم للعمل الجماعي ..او التبادل للخبرات والتقيات فيما بينهم .
وتجنيد عدد منهم كفيل بان يوصل تلك الشركات الأمنية لمعرفة اخر أساليبهم لغرض عمل ما يثبطها او يمنعها..

لكن تبقى مواكبة طبيعة احدث الهجمات الانترنت قاصرة وتبقى الكثير من الشركات الأمنية تعاني في عملها واهم مشكلة تعاني منها شركات الأمن الالكتروني هي مشكلة الوقت لأنهم حسب رأيهم يصممون أنظمة حماية وتعقب بعد ان يقوم هؤلاء المجرمون بأعمالهم التجسسية و الهجومية ..وبالتالي يغير هؤلاء الهكر تكتيكاتهم مرارا ويستخدمون ما هو جديد وفعال ..ثم تحاول الشركات الأمنية معرفته والسيطرة عليه او منعه...

وهكذا نجد ان هناك
حربا الكترونية بين
هؤلاء اللصوص
ومجرمي الانترنت
وشركات الأمن
المسؤولة عن حماية
بيانات غاية في
الخطورة والحساسية

المرجع:

http://www.elaphblog.com/posts.aspx?u=2548&A=61771

مشروع الحاسوب

عمل الطالبة : شيخة خليفة القريصي.

المستوى الحادي عشر.